NMCI AFCEA New Technology Abstract

Salutation	First Name	MI	Last Name	Suffix
	Paul	E	Secrest	

Company Name	Address	City, State	Zip Code	Country
World IT Solutions LLC	901 Brightseat Road	Landover, MD	20785-4725	USA

Telephone	Fax	E-mail	Website
301.843.8984	301.333.6230	CIO@witsllc.com	http://witsllc.com

Author Biography

Mr. Secrest served 20+ years in the Department of the Navy as a Surface Warrior and Naval Engineer. Mr. Secrest is a co-founder, Senior VP and Chief Information Officer for World IT Solutions (WITS) a service disabled, veteran-owned business.
WITS is a small business teaming partner on the NMCI Project. The WITS team provides a wide array of technical and Project Management professionals CONUS and OCONUS.
While serving at the President's Hospital, Mr. Secrest guided all of the National Naval Medical Center Information Technology (NNMC I.T.) Integration Projects as IT Department Head and Program Manager. He led network architecture functions and managed day-to-day operations of LAN/WAN, voice, video, and data networks systems and training. He implemented a team-centric defense-in-depth design for an Information Assurance (IA) Program using Department of Defense Information Technology Security Certification and Accreditation Process policies. This IA Program emphasized Policy, Preparation, and Vigilance backed up by industry best hardware.
Mr. Secrest was the Primary Design Architect for the District of Columbia Wilson Building Network Operations Center on a teaming Project with OAO Corp and DataNet, Inc. FY 2001.

Text

Computer networks are a critical and indispensable part of every government and military organization. EDS provided NMCI networks connect military networks to other private networks and the Internet to facilitate the real-time information exchange necessary for ongoing operations. While this connectivity and capacity for information exchange is required for work, it has the potential to be leveraged for the purpose of launching cyber attacks or cyber terror. Consequently, networked organizations must have the capability to react quickly to potential internal and external threats. Successful architecture for defending against threats should begin with security management that enables the following:

- Centralized management for implementing organization-wide security directives
- Distributed control for managing day-to-day operations and mitigating

conflicting organizational objectives within or between Communities of Interest(COI)

- Redundancy for disaster recovery
- Secure remote access to network resources
- Monitor and limit internal threats including those from returning or visiting deployable seats (laptops)

NMCI presently manually deploys IA rulebase and IAVA changes. Deploying centralized security management can expose conflicting objectives for government and military organizations. While headquarter locations prefer centralized control, divisions may want to retain some level of autonomy and local control. These conflicting organizational objectives can be a major roadblock for effectively implementing a security policy if they are not resolved. By building in controls for both NOCs and bases, it is possible to address these differing objectives and achieve effective policy management. Our brief will demonstrate how centralized management and internal threat monitoring can be seamlessly deployed over the NMCI network; achieving measurable real dollar cost reductions. This will include leveraging the existing already purchased NMCI Zone Lab personal firewalls into an intuitive, EAL-4 certified, centrally managed environment.